Project: implement length extension attack for SM3, SHA256, etc.

----这里我们选择 md5 进行攻击

代码说明：首先先从网上找一个 md5 的算法。接着开始进行长度拓展攻击：攻击原理为：MD5(IV，message+padding+append) = MD5(MD5(IV, message), append)，注意这里 append 填充规则里填充长度应该按照 message+padding+append 的填充长度，才能模拟 md5 内部状态

根据原理，我们可以先对 message 进行 MD5 加密，得到的输出再作为 IV 值输入到 MD5 加密算法中，再以我们要追加的 append 为密文输入加密，即可得到 message+padding+append 的 md5 结果

运行指导：直接运行 py 文件，

```
message = 'f357'
append='f47'
```

、

在输入变量中，message 假设信息未知，长度已知，append 可随意更改

运行结果截图：

```
message+padding+append 通过长度拓展攻击获得的md5为：  26b3c76769fbe026e9eee9691c96e1bd
message+padding+append 实际md5为：  26b3c76769fbe026e9eee9691c96e1bd
```